Int. J. on Recent Trends in Engineering and Technology, Vol. 9, No. 1, July 2013

Hierarchical Key Agreement Protocol for Wireless Sensor Networks

Ravi Kishore Kodali[1] and Sushant K. Chougule
National Institute of Technology, Warangal
Department of E.C.E., Warangal, India
[1]Email: ravikkodali@gmail.com

***Abstract*— Wireless sensor network promises ubiquitous data collection and processing for variety of commercial, healthcare and military applications. Practical realization of WSN applications is possible only after assuring network security. Cryptographic key distribution is an important phase in network security which establishes initial trust in the network. Security protocol implementation in WSN is limited by resource constrained nature of sensor nodes. The key distribution algorithm satisfying security requirements of given WSN application should be implemented with minimum communication and memory overhead. As a solution to this problem, hierarchical key management technique is proposed in this paper. Symmetric key pre-distribution technique with less computational overhead and ID-based asymmetric key (IBK) distribution technique with less communication overhead are applied simultaneously in the network at different levels. Resilience strength and resource overhead of the proposed scheme is compared with both symmetric and asymmetric techniques.**

***Index Terms*—WSN, ECC, Bilinear pairing, IBK, probabilistic key pre-distribution.**

I. Introduction

The technological advances in the wireless technology and the embedded systems have given rise to Wireless sensor networks (WSN's). WSN's are self- sustainable networks of tiny resource constrained sensor nodes. These tiny sensor nodes can play important role in data collection when collaborated with each other and connected to Internet. Recent work over 'Internet of things' considers WSN as a bridge between physical and virtual world. When applying WSN applications where many networks collaborate with each other, value of data collected by tiny sensor nodes is transcended. Such applications demand WSN with higher security level. But at the same time, because of energy and computational constraint of sensor nodes, security protocol with minimum overhead should be applied.

Fig. 1 shows the structure of hierarchical WSN. In WSN with flat topology, sensor nodes communicate with BS directly. However, in hierarchical topology, sensor nodes are grouped into clusters and only cluster heads communicates with BS after aggregating the data from the WSN nodes. The sensor nodes are deployed at remote and hazardous places, where the human intervention is not possible.

To track and monitor the event, the sensor nodes collaborate among themselves and pass the aggregated information to remote user through Base station (BS). BS is a network monitoring and controlling entity which acts as a mediator between sensor nodes and an authenticated remote user. In WSN, with a flat topology, sensor nodes communicate with the BS directly using multi-hop connectivity. However, in hierarchical topology, the nodes are grouped into clusters and only the cluster head communicates with the BS, after aggregating the data from sensor nodes. On the left side, functions of different levels are represented, while right side represents security issues of these levels.

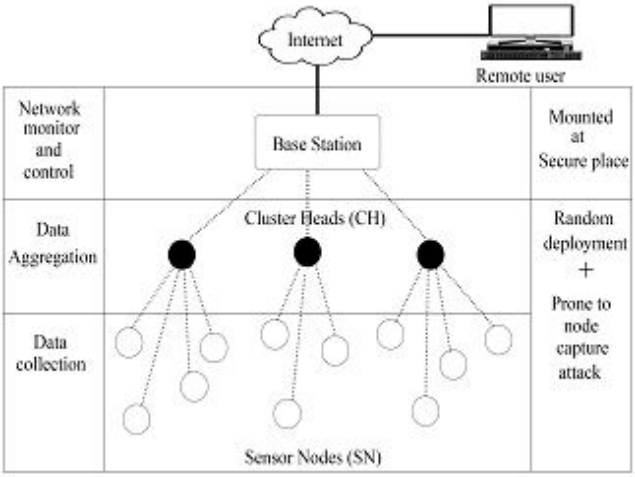

Figure 1. Security perspective of hierarchical WSN

As shown in Fig. 1, random deployment of sensor nodes in a remote area is prone to the node capture attack. Tamper resistant nodes and economical feasible and hence security protocol should take care of these kinds of attack. Also, the figure highlights that cluster head carries more important data than other nodes and hence security provided to CHs should be stronger. Wireless nature of WSN makes it more susceptible to eavesdropping. To deal with all these security issues, security protocol specific for WSNs is required.

Network security relies on symmetric cryptography, message authentication code and public key cryptography to provide confidentiality, integrity and authentication. Symmetric cryptography uses the same key to encrypt and decrypt data. Encryption assures confidentiality of data when it is transmitted through the link. To check the integrity of received data message authentication codes are used. But before encrypting the data with the symmetric cipher, parties involved in the communication should agree on a secret shared key. For this, a key exchange mechanism based on asymmetric cryptographic primitives can be used. In asymmetric cryptography, keys used for encryption and

DOI: 01.IJRTET.9.1.523

decryption are different. Server encrypts the secret key used in symmetric cipher with its private key and related public key is distributed to all the clients. The public key can be used to decrypt the symmetric key and subsequently the symmetric key is used for the further communication.

Cryptographic key management is fundamental part of network security. For wireless sensor network, because of their resource constrained nature, symmetric key pre distribution techniques were considered more suitable. With the advent of Elliptic curve cryptography many researchers explored the use of asymmetric key. Taking further the work on elliptic curve key exchange mechanism, Identity based key management makes use of bilinear pairing on elliptic curves. Even though identity based key management technique provides features like self authentication, on line key calculation, key update mechanisms and scalability, bilinear pairing function used in its key calculation intensively consumes computational resources. Hence, to provide solution to this problem hybrid key management technique is proposed in this paper. In the proposed scheme, identity based key management technique is applied to establish secure connection between the node in higher level of hierarchy i.e. cluster heads and base station. To secure the nodes in the lower level of hierarchy i.e. sensor node inside the cluster, pairwise probabilistic key pre distribution scheme is used. Section II, reviews the recent literature related to key management in wireless sensor networks. Section III provides mathematical background for proposed scheme and section IV discusses the proposed scheme in detail. Implementation of the scheme is discussed in section V. Section VI analyses the protocol thoroughly and presents the results. Section 7 concludes the paper and gives direction for future work.

II. Literature Review

Security of wireless sensor networks is critical aspect when their practical applicability and their new role in Internet of things [1] [2] is considered. To assure secure connectivity inside wireless sensor networks key management techniques plays important role. The Simplest way to establish key in WSN is to use single master key for the complete network. It provides full connectivity and scalability, but single node compromise can expose the whole network. To circumvent this problem, pairwise keys can be pre distributed in each node so that capturing the node will affect only single node keeping all other connections secure. But for WSN with N nodes, every single node should be loaded with (N 1) pairwise keys to achieve full connectivity. Apart from stringent memory requirement this technique limits the network scalability.

Probabilistic key pre-distribution scheme [3] strives to optimize connectivity and resilience against node capture attack. In this scheme, prior to node deployment, subset of keys from large key pool is stored into each node. Each key is tagged with unique identifier. Nodes broadcast key identifiers to their neighbors and pairwise key with the nodes having at least one common key. Nodes that are unable to establish direct pairwise key enters into secure path discovery phase. Node capture attack affects non-captured nodes as captured node contains common keys with given probability.

The probabilistic key pre distribution is improved in terms of security by Q composite random key distribution [4] which requires nodes to contain at least Q common keys to establish a pairwise key. This technique reduces the probability of compromising secured link between non captured nodes by the factor Q. Polynomial based pair wise key distribution scheme [5] keeps the network secure even until t nodes are captured, where is the order of polynomial. Polynomial $p(x,y)$ having coefficients over $GF(q)$ is used to establish keys between the nodes. The polynomial has the property $p(x,y) = p(y,x)$

$$p(x,y) = \sum_{0 \le i,j \le t}^{t} a_{ij} x^i y^j \quad (1)$$

where, a_{ij} are the elements of symmetric matrix A of order $t \times t$. Node with identity i stores $p(i,y)$ and to establish pair wise key with the node having identity j calculates stored polynomial over point j, $k_{i,j}$. Similarly node j computes pair wise key $p(j,y)$ over point i, $k_{j,i}$. Because of symmetry property of $A, k_{i,j} = k_{j,i}$. Matrix is the secret information in the network and $(t+1)/2$ nodes has to be compromised to calculate A.

Improvement in key pre distribution scheme can be obtained by combination of probabilistic key pre distribution, Q composite key generation and Polynomial pool based key pre distribution scheme [6]. Another key pre distribution challenge is posed by multi hop connectivity. Most of the key pre distribution schemes provide hop to hop secure links, but for better security end to end secure links between sensor and sink is required [7]. Well known data centric and location centric routing techniques are extended in [7] and applying differentiated key pre distribution end to end secure communication is achieved.

Key pre distribution schemes are based on security vs. connectivity trade off. Hence, to achieve both security and connectivity with minimum resource overhead many researchers have focused on asymmetric key establishment techniques suitable for Wireless sensor networks. Public key infrastructures (PKI) [8] used in computer networks requires Certification authority (CA) to bind the public key of user to its identity. Mechanism to handle large certificates and computationally intensive Digital Signature algorithms are too complex to implement on resource constrained WSN.

Public Key Infrastructure (PKI) can provide perfect connectivity and resilience. But Certification Authority (CA) is required to bind public of node to its identity. Shamir [9] first introduced Identity based encryption (IBE) scheme which uses unique ID of the device as its public key. For computer networks, this ID can be email address or IP address. In the context of WSN, ID can be assigned by network deploying

DOI: 01.IJRTET.9.1.523

party to ensure its uniqueness. Identity based key management (IBK) scheme does not require CA but another entity termed as Private key generator (PKG) takes node's ID and calculate respective private key. Research on ID based key techniques for WSN focus on Pairing based cryptography (PBC) to establish pairwise key between the sensor nodes. IBK protocol implementation for MANET and WSN is provided in [10] [11] [12]. ID based key management scheme is implemented in MANET with key refreshment technique [10]. Apart from $Setup, Extract, Encrypt$ and $Decrypt$ phases in IBE, $Refresh$ phase is added to update private keys after certain amount of time. This achieves Forward secrecy and dynamic key management. Taking this work further, $Refresh$, $Recover$ and $Revocation$ phases are added in ID based key management technique for WSN [12]. In their scheme more than one base stations are used to generate private key. In effect, this scheme achieves forward secrecy, backward secrecy, intrusion detection and resilience against base station capture attack. To achieve dynamic network topology, cluster formation and group key management techniques can be used along with key update and Revocation mechanism [11].

Resource Requirement of pairing algorithm when implemented on ARM processor is studied [13] using Pairing functions from MIRACL [14] library. Pairing is considered as the most power consuming operation. Results show that $0.444J$ power is consumed by pairing algorithm. Resource consumption in terms of energy and processing time of arithmetic operations over super singular elliptic curve is also presented. TinyPBC [15] is pairing algorithm which provides identity based key management without interaction between participating nodes. The paper shows that a MICA2 sensor node with ATmega128L micro controller $(8-bit/7.3828MHz)$ computes pairings in $5.5s$ time. K. McCusker [16] presented symmetric key distribution scheme based on Identity based cryptography (IBC). The asymmetric key algorithm (IBC) for authenticated key agreement and then encryption can be performed using symmetric keys generated. An accelerator hardware for Tate pairing achieves running time of $1.75ms$ and energy consumption of $0.08mJ$. These are the best result in the field of ID based key management scheme for WSN. Balance between resilience and resource consumption between nodes can be achieved by applying both symmetric and asymmetric key distribution techniques in hierarchical wireless sensor network [17].

For heterogeneous wireless sensor network, key management technique based on AVL tree [18] and ECC is used to distribute keys with minimum resource requirement [19]. Cluster formation is secured using master public/pair key calculated using elliptic curve. Since cluster heads, Leader nodes with durable batteries are decided prior to deployment flexibility in random deployment of the network is lost. Framework for key pre-distribution scheme for heterogeneous wireless sensor networks is discussed in [20]. The problem of distributing the keys to different types of nodes is analyzed. The scheme does not consider the hierarchical WSN. Group key distribution technique for hierarchical WSN is proposed in [21]. Different types of group keys for nodes at different levels are established after deployment. The scheme is tested with on hardware platform with TinyOS operating system. ECC-based key management technique for hierarchical WSNs is proposed in [22]. Signcryption technique is used to secure channel between Cluster lead and base station to provide forward secrecy. To circumvent the problem of node compromise, period authentication of sensor nodes is done.

III. Mathematical Background

Bilinear pairing is the integral part of Identity based key management scheme and for design of secure key establishment good understanding of bilinear pairing properties is required.

A. Bilinear pairing

Definition: Bilinear pairing is a map of additive groups G_1 and G_2 to multiplicative group G_T

$$G_1 \times G_2 \rightarrow G_T \tag{2}$$

Based on groups G_1 and G_2 there are three types of pairings [23].

1. $G_1 = G_2$

2. $G_1 \neq G_2$, there exist an efficiently computable homomorphism, $\phi : G_2 \rightarrow G_1$

3. $G_1 \neq G_2$, ϕ does not exist

Type 1 and Type 2 pairings are similar and considered as same type. In Type 3 pairing, since mapping between and does not exist, it is difficult to get security proof for the pairing application.

Algorithm 1

Input: $P, Q \in E$, where P has order n

Output: $e\,(P, Q)$

Choose suitable point $R \in E$

$Q' \leftarrow Q + R$

$T \leftarrow P$

$m \lfloor log_2(n) \rceil - 1, f \leftarrow 1$

while $m \geq 0$ **do**

Calculate lines l and v for doubling T

$T \leftarrow [2]T$

$f \leftarrow f \dfrac{l(Q')v(R)}{v(Q')l(R)}$

if $n(m) = 1$ **then**

Calculate lines l and v for addition of T and $P0$

$T \leftarrow P$

$f \leftarrow f \dfrac{l(Q')v(R)}{v(Q')l(R)}$

DOI: 01.IJRTET.9.1.523

end if

$m \leftarrow m - 1$

end while

return $f \leftarrow f^{\left(\frac{q^k-1}{n}\right)}$

Hence, Type 1 and Type 2 pairings are more suitable for WSN applications. Also for resource constrained WSN applications, selection of G_1 should be such that there exist short representation of elements in G_1 . Key establishment protocol is based on following properties of bilinear pairing.

Bilinearity: For $P, R \in G_1$ and $Q, S \in G_2$,

$$e(P+R,Q) = e(P,Q)e(R,Q)$$
$$e(P,Q+S) = e(P,Q)e(P,S) \quad (3)$$

Hence consequently, for $a, b \in Z$

$$e(a.P,Q) = e(P,Q)^a = e(P,a.Q)$$
$$e(P,b.Q) = e(P,Q)^b = e(b.P,Q) \quad (4)$$

Non degeneracy: $\forall P \in G_1$ there exists $Q \in G_2$ such that

$$e(P,Q) \neq 1 \quad (5)$$

Weil and Tate pairing are popular pairing algorithms and can be calculated using Miller algorithm [24]. Weil pairing is simple to understand and implement. However, two iterations of Miller algorithm are required for Weil pairing and consume more time than Tate pairing which requires single iteration of the Miller algorithm. Tate pairing computation using Miller algorithm is given in Algorithm 1 [25]. (v and l represents vertical and horizontal line respectively).

B. Pairing friendly curves

Bilinear pairing operations are based on elliptic curves with given parameter. For the success of pairing based cryptographic algorithm, selection of elliptic curve parameters is crucial task. Algorithms to calculate pairing friendly curves over prime order field (q) based on Complex Multiplication (CM) method are discussed in [26] and [27]. Main objective of these algorithms is to calculate elliptic curve parameters such that embedded degree k [25] is kept smaller for larger prime fields. Acceptable values of over prime field are $(4, 6, 12)$. If pairing is implemented on super-singular elliptic curves, computational cost is reduced. But for large prime field k is restricted to which is not sufficient to satisfy security requirements corresponding to Discrete logarithm problem (DLP) in F_{q^k}. Hence, non prime order fields of characteristics 2 and 3 $(2^s, 3^s)$ are helpful in case of super-singular curves $(k = 3, 4, 6)$ [23]. Open source cryptographic library TinyPairing [28] implements pairing over characteristic-3 field $(F_{3^{97}})$ and same is used for implementation of proposed key management scheme.

IV. SCHEME

The proposed scheme is an application of symmetric and asymmetric key management techniques at different levels of sensor nodes. Hierarchical sensor network is considered in which every cluster one sensor node with the duties of cluster head has. Cluster head exchange aggregated data from sensor nodes with other cluster heads and base station. Hence, information at cluster head level has transcended value and security at this level must be stronger. Identity based key establishment is applied among the cluster heads and base station. Sensor nodes inside the cluster are more in number and computationally lightweight probabilistic key pre distribution technique is applied inside cluster. Security threats of probabilistic key pre distribution technique are kept limited to cluster. The proposed key management technique aims at reducing energy consumption of entire network by balancing resilience and computational cost of the key management protocol.

A. Setup

The execution of the proposed key management protocol requires security primitives to be installed in sensor node prior to deployment. For probabilistic key pre- distribution scheme, key ring from large key pool is stored. At the same time, to execute Identity based key establishment protocol, pairing function also should be in each node since cluster head is altered periodically. Following mathematical functions and key pre-distribution material is installed in each node prior to deployment:

- $ID_i \leftarrow$ Self identity of node *i*
- $E \leftarrow$ Elliptic curve parameters of pairing friendly elliptic curve
- $e(p, q) \leftarrow$ Bilinear pairing function between p and q
- $H_1 \leftarrow$ Hash function to map identity of node to its public key
- $H_2 \leftarrow$ Hash function to map pairing output to cryptographic key
- $ID_list \leftarrow$ List of the identities of nodes in the entire network
- $k_{ring} \leftarrow$ Subset of keys from large key pool S with unique identifiers

The proposed key management protocol is implemented over sensor nodes using TinyOS operating system and hence TinyOS image is also dumped on sensor node. Master secret key s is generated and stored on Base station. Deployment of nodes is not dependant on pre-distributed material which adds flexibility to scheme. Fig.2 illustrates secure cluster formation.

B. Hierarchical network formation

The proposed key management scheme is designed for wireless sensor network with hierarchical topology. Formation of clusters in secure way is essential to isolate the security threats within the given cluster. Base station (BS) initiates the process of cluster formation by broadcasting HELLO message. Sensor node responding first to BS is selected as cluster head (CH). BS provides corresponding private key to CH and broadcast CH's ID to all the nodes. CH forms a cluster with its neighboring nodes and sends list of IDs in the cluster

DOI: 01.IJRTET.9.1.523

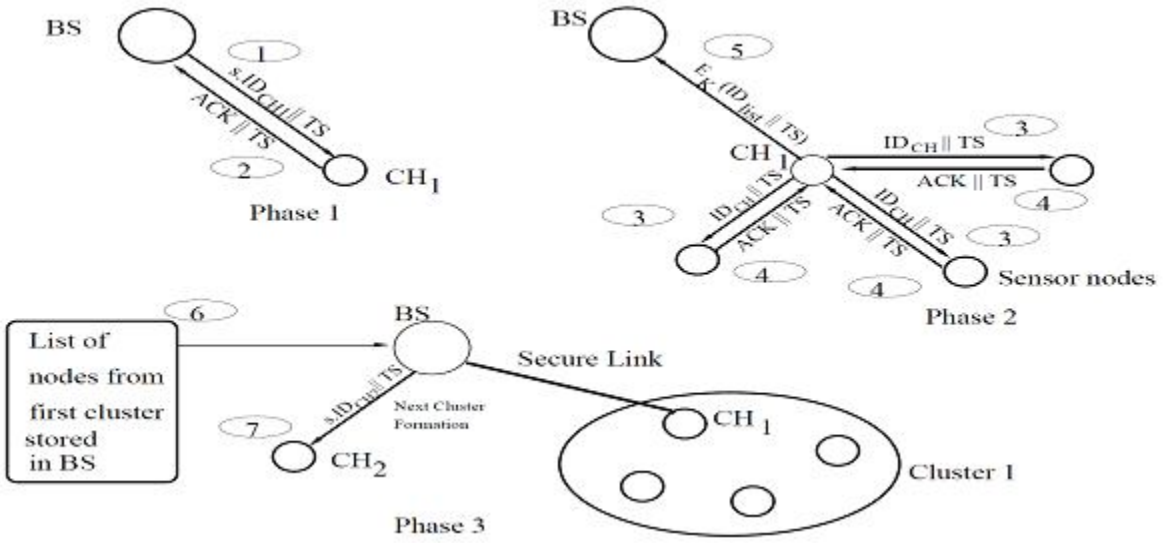

Figure 2. Secure cluster formation

to BS. All the messages are attached with Time stamp (TS) to avoid Replay attack and presented in (7).

$$BS \rightarrow Broadcast : HELLO$$

$$BS \leftarrow CH : ACK||TS$$

$$BS \rightarrow CH : s.ID_{CH}||TS$$

$$BS \rightarrow Broadcast : ID_{CH}||TS$$

$$CH : e(s.ID_{CH}, ID_{BS}) = K_{CH-BS}$$

$$CH \rightarrow Broadcast : ID_{CH}||TS$$

$$CH \leftarrow SN : ACK||TS$$

$$BS \leftarrow CH : Encrypt_{K_{CH-BS}}(ID_{list}||TS) \quad (6)$$

It should be noted that Encrypt function used at the last stage can be any symmetric cipher algorithm.

C. Identity based key establishment

Use of bilinear property allows non interactive key distribution between a pair of cluster heads. Since Identity of node is mapped to public key, Certification authority is not required. However, private key generator (PKG) is required and Base station acts as PKG. Security of key establishment depends on discrete logarithm problem of bilinear pairing. Fig. 3 illustrates Identy based key agreement.

D. Intra cluster key management

Inside the cluster, keys are established between cluster head and sensor nodes using key ring set pre installed on sensor nodes. Cluster head initializes key establishment by broadcasting its key identifier list. Sensor nodes inside CH's communication range response to it by sending key identifiers of shared keys. Nodes not sharing the keys with the CH directly are securely connected with CH by path key establishment. CH isolates the sensor nodes inside its cluster by key reinforcement and the same is depicted in (7).

$$K_{CH-Node} \leftarrow H_2(K_{CH_i} \oplus k_{CH-Node}) \quad (7)$$

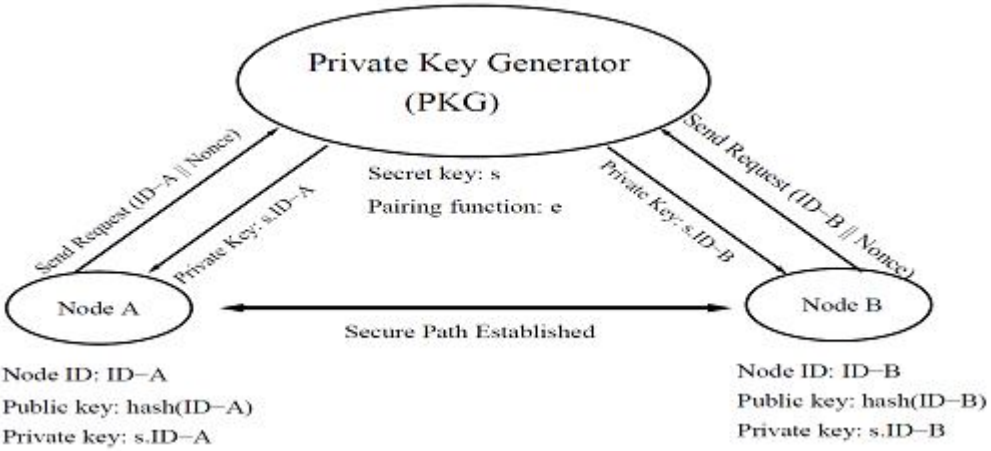

Figure 3. Identity based key agreement

DOI: 01.IJRTET.9.1.523

If sensor node is not able to establish intra cluster key even after shared key search and path key establishment, CH takes list of key identifier's from the node's key ring and pass it to contiguous CHs. The last step adds to communication overhead and advisable only when 100 percent connectivity is required.

E. Key update

The key update mechanism is an essential part of key management technique to protect the network from the removed nodes and from adversary which is doing traffic analysis for long time duration. The most desired characteristic of key update mechanism is to generate the updated key completely independent from the old key. In the proposed scheme, cluster heads are altered periodically. Consequently, keys associated with the CHs are also updated. Alteration of CHs achieves dual purpose of energy conservation and respective key updates. Cluster head alteration is initialized by old cluster head. It sends Energy level request message to all nodes in its cluster. Node having the highest energy level is selected as new cluster head. The key update takes place as shown in the fig. 4.

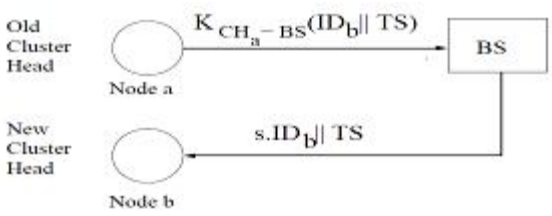

Figure 4. Key update mechanism for CHs

V. Protocol Implementation

The key management protocol is implemented for micaz [29] sensor motes with TinyOS operating system [30]. TinyOS is an embedded operating system, specially designed for resource constrained sensor nodes. TinyPairing [28] cryptography is written in nesC language and it is used for pairing algorithm required for Inter cluster key agreement. Elliptic curve is defined over non prime field of $F_{3^{97}}$ and embedded degree (k) is 6. Output of pairing is shared key between two nodes and it is an extended field element of size 624 bits. This field element is hashed to cryptographic key of desired size $(80bits, 128bits, 256bits)$ and extended field element is discarded to save the memory.

TinyOS application of key management protocol is written in nesC and targeted for Micaz sensor mote which consist of ATMEGA 1281 micro-controller [31] atmega1281 and RF230 transceiver chip [32]. Atmega1281 has 128 KB of ROM and 8 KB of RAM which proved sufficient for proposed key management protocol with memory left for other sensing and routing applications.

Communication messages passed among the nodes plays important role, because communication overhead directly depends upon these messages. For intra cluster key establishment following message is broadcast by cluster head.

Counter	**Type**	ID_{CH}	**Key identifier list [** k_{ring}**]**

Size of the message for $k_{ring} = 80$ $(p = 0.5)$ is 163 Bytes. Identity based key agreement requires private key to be transmitted from BS to CH. It is communicated through following message.

TABLE I. COMMUNICATION OVERHEAD ANALYSIS

Key scheme	Key ID broadcast	Path Key Discovery	Private key sharing	Total
Probabilistic pre-distribution	240 B per node	240 B per alternate node	-	352 KB
IBK	-	-	16 B per node	16 KB
Hybrid	240 B per CH	240 B per alternate node in cluster	16 B per CH	120 KB

Counter	**Type**	ID_{CH}	**Private key** $s.ID_{CH}$

Size of the message is 31 Bytes. Other than these messages 'HELLO' and 'ACK' messages are passed between the nodes. It should be noted that given messages are defined at application level and MAC layers frames are constructed according to IEEE 802.15.4 protocol.

VI. Results and Analysis

A. Analysis of key management scheme

Different key management related issues of the proposed hybrid key technique are discussed as follows:

Scalability: Cluster head formation mechanism adopted in the scheme allows large sensor nodes to be deployed with minimum overhead on the memory and energy resources. Cluster head formation mechanism is secure and because of on line key calculation mechanism new clusters can be easily added at any phase of network lifetime.

Forward and backward secrecy: Because of periodic Cluster head alteration secret keys related to each cluster are updated regularly and hence new nodes cannot detect previous messages. Key reinforcement assures that keys related to sensor nodes in lower level of hierarchy are also updated.

Communication overhead: In ID based key distribution, public key is nothing but the node identity, which is stored in each node for routing purpose. Also, bilinear pairing allows non interactive key distribution between the two nodes. In this way, Non interactive key establishment using ID based cryptography minimizes communication overhead. However, communication overhead is implied by shared key and path key discovery inside the cluster. Table I shows total bytes communicated in the network.

Memory overhead: Memory overhead of the proposed

DOI: 01.IJRTET.9.1.523

scheme is more than that of probabilistic key distribution and Identity based key management techniques. Reduced computational and energy cost is compensated with additional memory overhead. Table II compares the memory overhead of IBK, probabilistic key pre distribution and proposed hybrid scheme.

TABLE II. MEMORY OVERHEAD

	Probabilistic	IBK	Hybrid
Memory Overhead	2176 B	48 KB	50.125 KB

Energy consumption: Cluster head consumes most of the energy and there is a chance of single node energy drain out. In the proposed scheme, energy consumption is distributed among all the nodes as cluster head is altered periodically. WSN is considered as single entity and accordingly energy conservation methods are implemented. Simple key pre-distribution technique is applied for majority of the nodes in the network, which requires less energy compared to IBE. Also, energy is conserved by non interactive key calculation at cluster head level.

B. Resilience against node capture attack

In WSN, sensor nodes are openly distributed on the field and chances of node capture are more. When node is captured in case of probabilistic key pre distribution scheme, secret information related to non captured nodes is also revealed. In Identity based key management technique, communication links between non captured nodes are not compromised because of discrete logarithmic problem imposed by bilinear pairing. In Hybrid key management technique, communication links between non captured nodes inside the cluster are affected. Key reinforcement assures that communication links outside the cluster are not compromised. Fig. 5 shows the same comparison of the resilience against node capture attack. The parameters used to analyze the proposed key management are given in Table III.

For probabilistic key distribution technique, connectivity analysis is carried out by both simulation and theoretical calculation and the same is shown in fig. 6. Following parameters are considered for the analysis:

- Randomly generated large key pool size, P:10000
- Key ring size, k: 10 to 100
- Number of nodes in the network, n: 200
- Number of nodes in a cluster, n': 20

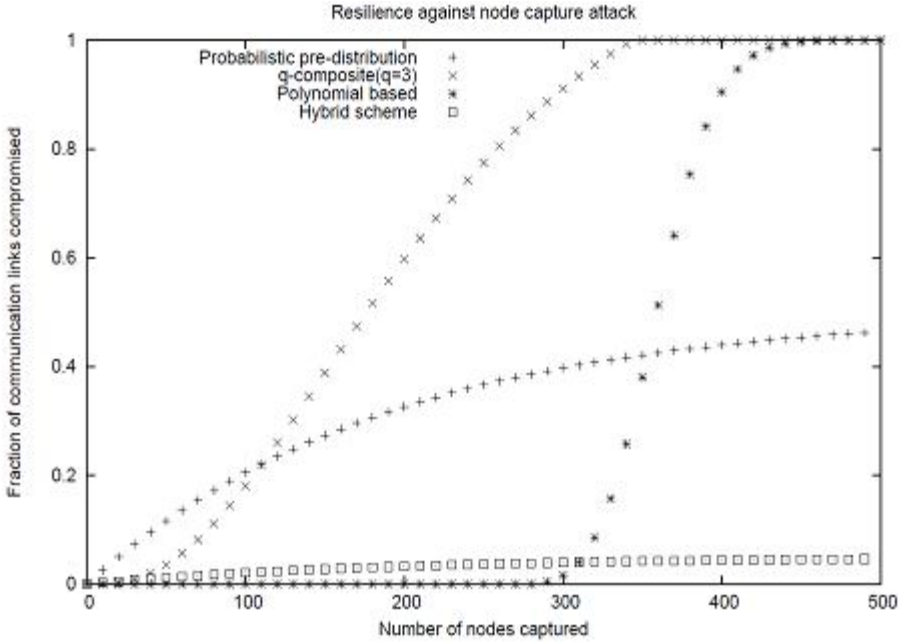

Figure 5. Analysis of resilience against node capture attack

TABLE III. SIMULATION PARAMETERS FOR RESILIENCE ANALYSIS

Simulation parameter	Value
Number of nodes in WSN	1000
Number of nodes captured	0 to 500
Number of clusters	10
Connectivity probability	0.5
Key pool size	120

CONCLUSIONS

Key management in a network is important while implementing any security protocol. Both symmetric key pre-distribution and asymmetric key distribution techniques fail to provide required security level using permissible resource overheads in WSN's. In heterogeneous WSN's, solution to solve this problem by implementing hybrid key management technique is analyzed. Both the computational and energy costs are reduced at the expense of memory overhead. The

DOI: 01.IJRTET.9.1.523

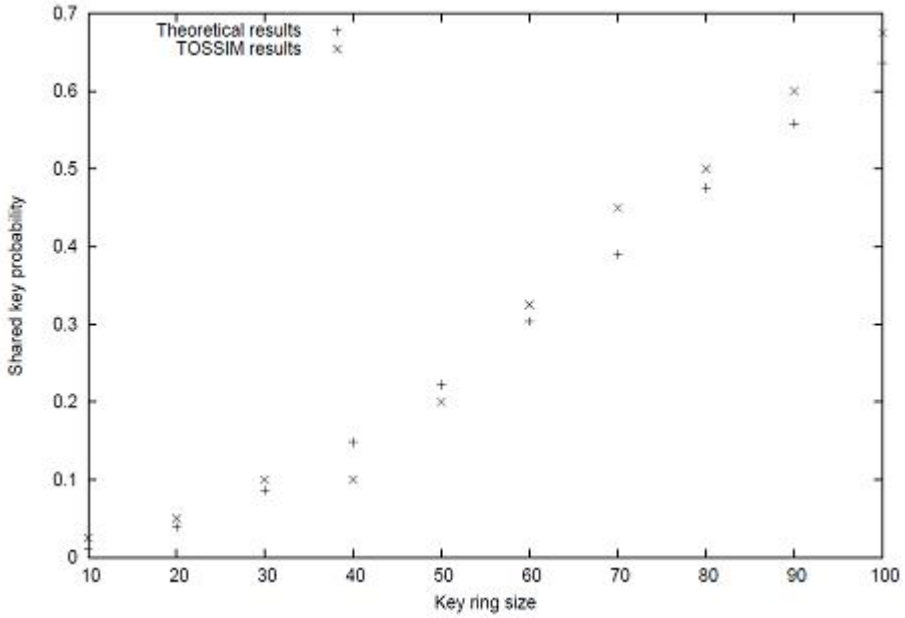

Figure 6. Simulation results for connectivity of probabilistic key distribution

communication overheads of the proposed scheme are moderate and efforts can be taken to reduce the same. Resilience against node capture attack of hybrid key management scheme is improved compared to probabilistic key pre-distribution techniques. The key reinforcement mechanism assures that security limitations of key pre-distribution technique are kept limited within the cluster.

References

[1] L. Atzori, A. Iera, and G. Morabito, "The internet of things: A survey," *Computer Networks*, vol. 54, no. 15, pp. 2787–2805, 2010.

[2] R. Roman, C. Alcaraz, J. Lopez, and N. Sklavos, "Key management systems for sensor networks in the context of the internet of things," *Computers & Electrical Engineering*, vol. 37, no. 2, pp. 147–159, 2011.

[3] L. Eschenauer and V. Gligor, "A key-management scheme for distributed sensor networks," in *Proceedings of the 9th ACM conference on Computer and communications security*. ACM, 2002, pp. 41–47.

[4] H. Chan, A. Perrig, and D. Song, "Random key predistribution schemes for sensor networks," in *Security and Privacy, Proceedings. 2003 Symposium on*. IEEE, 2003, pp. 197–213.

[5] R. Blom, "An optimal class of symmetric key generation systems," in *Advances in Cryptology*. Springer, 1985, pp. 335-338.

[6] Rasheed and R. Mahapatra, "Key pre-distribution schemes for establishing pairwise keys with a mobile sink in sensor networks," *Parallel and Distributed Systems, IEEE Transactions on*, vol. 22, no. 1, pp. 176– 184, 2011.

[7] W. Gu, N. Dutta, S. Chellappan, and X. Bai, "Providing end-to-end secure communications in wireless sensor networks," *Network and Service Management, IEEE Transactions on*, vol. 8, no. 3, pp. 205–218, 2011.

[8] S. William *et al.*, *Cryptography and Network Security, 4/e*. Pearson Education India, 2006.

[9] Shamir, "Identity-based cryptosystems and signature schemes," in *Advances in cryptology*. Springer, 1985, pp. 47–53.

[10] S. Balfe, K. Boklan, Z. Klagsbrun, and K. Paterson, "Key refreshing in identity-based cryptography and its applications in manets," in *Military Communications Conference, 2007. MILCOM 2007. IEEE*. IEEE, 2007, pp. 1–8.

[11] J. Jian-wei and L. Jian-hui, "Research on key management scheme for wsn based on elliptic curve cryptosystem," in *First International Conference on Networked Digital Technologies, 2009. NDT'09*. IEEE, 2009, pp. 536–540.

[12] S. Saab, A. Kayssi, and A. Chehab, "A decentralized energy-aware key management scheme for wireless sensor networks," in *Internet Technology and Secured Transactions (ICITST), 2011 International Conference for*. IEEE, 2011, pp. 504–508.

[13] B. Doyle, S. Bell, A. Smeaton, K. Mccusker, and N. O'Connor, "Security considerations and key negotiation techniques for power constrained sensor networks," *The Computer Journal*, vol. 49, no. 4, pp. 443–453, 2006.

[14] M. Scott, "Miracl–multiprecision integer and rational arithmetic c/c++ library," *Shamus Software Ltd, Dublin, Ireland, URL¡ http://www. Shamus.ie*, 2003.

[15] L. Oliveira, M. Scott, J. Lopez, and R. Dahab, "Tinypbc: Pairings for authenticated identity-based non-interactive key distribution in sensor networks," in *Networked Sensing Systems, 2008. INSS 2008. 5th International Conference on*, june 2008, pp. 173 –180.

[16] K. McCusker and N. O'Connor, "Low-energy symmetric key distribution in wireless sensor networks," *Dependable and Secure Computing, IEEE Transactions on*, vol. 8, no. 3, pp. 363 –376, may-june 2011.

[17] M. Rahman and S. Sampalli, "A hybrid key management protocol for wireless sensor networks," in *Trust, Security and Privacy in Computing and Communications (TrustCom), 2012 IEEE 11th International Conference on*. IEEE, 2012, pp. 769 776.

[18] Y. Y. Zhang, W. C. Yang, K. B. Kim and M. S. Park, "An avl tree-based dynamic key management in hierarchical wireless sensor network," in *International Conference on Intelligent Information Hiding and Multimedia Signal Processing, 2008. IIHMSP'08*. IEEE, 2008, pp. 298–303.

DOI: 01.IJRTET.9.1.523

[19] H. Boumerzoug, B. Amar Bensaber, and I. Biskri, "A key management method based on an avl tree and ecc cryptography for wireless sensor networks," in *Proceedings of the 7th ACM symposium on QoS and security for wireless and mobile networks*. ACM, 2011, pp. 57–62.

[20] K. Lu, Y. Qian, M. Guizani, and H.-H. Chen, "A framework for a distributed key management scheme in heterogeneous wireless sensor networks," *Wireless Communications, IEEE Transactions on*, vol. 7, no. 2, pp. 639–647, 2008.

[21] B. Panja, S. Madria, and B. Bhargava, "Energy and communication efficient group key management protocol for hierarchical sensor networks," in *Sensor Networks, Ubiquitous, and Trustworthy Computing, 2006. IEEE International Conference on*, vol. 1, 2006, pp. 8.

[22] M. Alagheband and M. Aref, "Dynamic and secure key management model for hierarchical heterogeneous sensor networks," *Information Security, IET*, vol. 6, no. 4, pp. 271–280, 2012.

[23] S. D. Galbraith, K. G. Paterson, and N. P. Smart, "Pairings for cryptographers," *Discrete Applied Mathematics*, vol. 156, no. 16, pp. 3113–3121, 2008.

[24] V. S. Miller, "The weil pairing, and its efficient calculation", *Journal of Cryptology*, vol. 17, no. 4, pp. 235–261, 2004.

[25] Blake, G. Seroussi, N. Smart, and J. Cassels, Advances in Elliptic Curve Cryptography (London Mathematical Society Lecture Note Series). Cambridge University Press, 2005.

[26] Miyaji, M. Nakabayashi, and S. Takano, "New explicit conditions of elliptic curve traces for fr-reduction," *IEICE transactions on fundamentals of electronics, communications and computer sciences*, vol. 84, no. 5, pp. 1234–1243, 2001.

[27] P. S. Barreto and M. Naehrig, "Pairing-friendly elliptic curves of prime order," in *Selected areas in cryptography*. Springer, 2006, pp. 319–331.

[28] X. Xiong, D. S. Wong, and X. Deng, "Tinypairing: a fast and lightweight pairing-based cryptographic library for wireless sensor networks," in *Wireless Communications and Networking Conference (WCNC), 2010 IEEE*. IEEE, 2010, pp. 1–6.

[29] M. Datasheet, "Crossbow technology inc," *San Jose, California*, 2006.

[30] P. Levis, S. Madden, J. Polastre, R. Szewczyk, K. Whitehouse, A. Woo, D. Gay, J. Hill, M. Welsh, E. Brewer *et al.*, "Tinyos: An operating system for sensor networks," *Ambient intelligence*, vol. 35, 2005.

[31] Atmega128, "8-bit microcontroller datasheet. 2003," *USA, California: Atmel Corporation*.

[32] M. CC2420, "2.4 ghz IEEE 802.15. 4/zigbee-ready rf transceiver specification. January, 2006

DOI: 01.IJRTET.9.1.523